Aperia

PCI Apply MS User's Guide

V4.1

August 17, 2021

Contents

Introduction 5
Overview 5
Types of Merchants 5
Master Merchants and Chaining Accounts 6
PCI Compliance Process 6
Reports 8
Reading Conventions 8
Glossary 9
Access PCI Apply 9
Log In 9
First Time Log In 10
Retrieve Forgotten Username 10
Reset Forgotten Password 11
Log Off 11
Navigation and General Functions 11
Toolbar and Menu 11
General Functions and Appearance 12
Links to Other Information 12
Additional Information Icon 12
Resources 12
Documents 13
Education 13
FAQs 13
Glossary 14
Landing Page 14
Merchant Information 15
Verify the Merchants Chained to Your Master Account 15
Verify Your Merchant Information 16
Certify Merchants Chained to Your Master Account 18

Accept Master Merchant Status 18
Questionnaire Selection 18
Questionnaire Descriptions 19
Select a Questionnaire 21
Questionnaire 22
Questionnaire Status 22
Complete a Summarized Questionnaire 23
Complete a Full Questionnaire 23
Network Scan 24
Scan Process 24
ASV Compliance Status 25
Enter Your Scan Targets 26
Manually Enter Scan Targets 26
Import Scan Targets 27
Verify Scan Targets 27
Identify the Scan Targets in the Scan Scope 29
Launch an ASV Scan 29
Schedule Scans 31
Schedule Scans on Specific Date 31
Schedule Recurring Scans 32
Edit a Scan Schedule 32
Disable a Schedule 33
Launch a Scan for Targets with Scheduled Scans 33
Respond to the Scan Results 33
Respond to Fail – Action Needed Status 33
Respond to Action Required Status 36
ASV Compliance Request 37
Submit an ASV Compliance Request 37
Review Your Compliance Request 39
Respond to a Declined Compliance Request 39
Download Your Compliance Reports 40

Download the Attestation of Scan Compliance Report....40
Download the Executive Summary and Vulnerability Details Reports....40
Review and Sign....41
Review and Sign Your Compliance Questionnaire....41
Get Your Site Seal....41
Reports....42
Additional Security Services....42
Endpoint Management....42
Endpoint Protection....43
Keystroke Encryption....43
Endpoint Scanning....43
Scan a Device....44
Send a Scan Inquiry to Another Device....44
Data Breach Protection....44

Introduction

This user's guide contains the essential information you need to use the PCI Apply application. It provides an overview of the PCI Compliance validation process and detailed information on how you use PCI Apply to attest to your compliance.

This guide is intended for merchants and merchant support personnel who are responsible for their organization's PCI compliance.

Due to the sensitivity of the information included in this document, under no circumstances should this document be disclosed to any parties that are not directly involved in the testing or use of the Aperia PCI Apply.

Overview

Payment card industry (PCI) compliance is mandated by credit card companies to help ensure that credit card payments and related transactions are secure. Businesses that accept credit card payments (merchants) must follow technical and operational standards established by the PCI Security Standards Council. Adhering to the Payment Card Industry Data Security Standards (PCI DSS) helps you secure and protect the credit card data provided by cardholders and transmitted through credit card transactions. When you demonstrate your consistent adherence to the PCI DSS, you are said to be in compliance.

This document contains information about how to use PCI Apply to attest to your compliance. This document does not contain information about the PCI DSS requirements or what you must do to meet those requirements. However, you may access information about those requirements from within the PCI Apply application.

To be in compliance, you must complete an appropriate self-assessment questionnaire (SAQ) annually. If you are using a qualified method of accepting payments, then you also must have your website or terminal scanned and approved for compliance quarterly. This must be done by a PCI SSC approved scan vendor (ASV).

Types of Merchants

- Online Merchants: You are an online merchant if you use PCI Apply to attest to your compliance.
- Offline Merchants: You are an offline merchant if you gave a paper copy of your current, completed SAQ to your acquirer or other PCI provider. Usually, this is because you are transferring to new PCI provider after completing your current compliance attestation with another PCI provider. Your PCI provider will have

identified your offline status and your compliance status. Your PCI provider may also have uploaded your compliance documents into PCI Apply. Your status will change to online when your current compliance expires, and you will complete your next compliance attestation in PCI Apply.

- Third-Party QSA Merchants: You are a third-party QSA merchant if your compliance validation document was provided to your acquirer or other PCI provider by a qualified security assessor (QSA) entity. Your compliance validation document may be a report on compliance (ROC) or an SAQ.

Master Merchants and Chaining Accounts

A merchant business which has more than one location or profit center may have a merchant ID for each of those locations or profit centers. If you have multiple merchant IDs and they all process credit cards using the same payment methods, processing procedures, and security policy, your PCI provider may have associated your merchant IDs into a chain. This enables you to attest to compliance for all the chained merchant IDs at one time.

You will attest to compliance through the master merchant ID for the chain. The other merchant IDs in the chain are identified as associated merchants. You cannot enter or change information for associated merchants in your chain. You can, however, view each associated merchant's information and compliance status.

PCI Compliance Process

PCI Apply leads you through the compliance process, and it shows your status and where you are in the process. You must complete the PCI DSS self-assessment questionnaire (SAQ) required for your business environment once a year.

Your payment processing method and SAQ may require a scan of your network, called an ASV scan. If an ASV scan is required, then you must conduct the scan and have the results approved every 90 days. This must be done by a PCI SSC approved scan vendor (ASV).

Aperia and your PCI provider recommend that you do not wait until the end of a 90-day period to start the scan process. The scan may take some time to complete, and it may reveal issues that you must address to get approval.

At a high-level, the process for attesting your compliance is:

1. Verify your merchant information.
2. Complete the required PCI DSS self-assessment questionnaire. You must do this annually.

3. Complete an ASV scan, if required by your self-assessment questionnaire. When scanning is required, you must complete a scan every 90 days.
4. Review and sign your questionnaire. If your questionnaire does not require a scan, you can do this as soon as you complete the questionnaire. If your questionnaire requires a scan, then you can do this once your first quarterly ASV compliance request is approved by the ASV team.

Self-Assessment Questionnaire

The self-assessment questionnaire (SAQ) enables you to attest to your own PCI DSS compliance. There are several SAQs for different business environments and methods of processing payments. You must complete the questionnaire that is applicable to your business. You will sign and submit your completed questionnaire as part of your attestation of compliance.

The SAQs for some business environments and methods of payment require that you perform an ASV scan of your network every 90 days.

ASV Compliance

As part of your PCI attestation of compliance, you may be required to complete an external vulnerability scan of your computer network to validate your adherence to the external requirements of PCI DSS Requirement 11.2.2.

PCI DSS requires a vulnerability scan every 90 days of the externally accessible, internet-facing network components that are part of your card processing network or that may provide access to it. You must also provide all fully qualified domain names that are entryways into your entire in-scope card processing network. These include, but are not limited to:

- Domains for web servers
- Domains for mail servers
- Domains used in name-based virtual hosting
- Web server URLs to hidden directories that cannot be reached by crawling the website from the home page
- Any other public-facing hosts, virtual hosts, domains or domain aliases

You must define and attest to your scan scope when submitting your ASV compliance request. You are responsible for defining the appropriate scope of your scan and providing all your internet-facing IP addresses and domain names for scanning. You are responsible if an account data compromise occurs via an externally facing system component that you did not include in your scan scope.

The scan must be performed by an approved scanning vendor (ASV). PCI Apply gives you access to the Aperia ASV service, which is approved by the PCI Council. Aperia conducts external vulnerability scanning services to validate your adherence to the PCI DSS external requirements.

You must complete an ASV scan once every 90 days. Because scanning can take some time, Aperia recommends that you complete a scan before your 90-day period expires. You should also check any changes you have made to your credit card processing system prior to starting a scan.

Your ASV compliance request must be reviewed and approved by the Aperia ASV team.

Reports

PCI Apply generates reports as you complete the compliance attestation process. These reports are available from PCI Apply for at least three years, as required by the PCI council. You may download or print a copy of your PCI documents to file for your company records.

Reading Conventions

Convention	Meaning
Text in this format	Identifies active user interface elements including: ▪ Button names ▪ Commands on menus, toolbars, and ribbons ▪ Dialog box options ▪ Icon names ▪ List names ▪ Tab names
Text in this format	Indicates a key on the keyboard. For example, press **Enter**, or press **Tab**.
Text in this format	Indicates a note that emphasizes or supplements important points of the main text or that gives a tip to help you apply the techniques and procedures described.
Text in this format	Indicates a caution note, which advises you that failure to take or to avoid a specific action could result in loss of data.

Convention	Meaning
Text in this format	Indicates an important note, which provides information is essential to the completion of a task.

Glossary

Term	Definition
AOC	Attestation of compliance
ASV	Approved scanning vendor
Moto	Mail order/telephone order
MRI	Merchant relation indicator
PCI	Payment card industry
QSA	Qualified security assessor
ROC	Report on compliance
SAQ	Self-assessment questionnaire

Access PCI Apply

PCI Apply operates within the following web browsers: Microsoft Internet Explorer, Firefox, and Google Chrome. Please note that the application is optimized for a screen resolution of 1280x1024. The application may appear differently on a mobile device.

Log In

If you have a username and password (including a temporary password), use this process to log into PCI Apply. If you do not have a username and password, use the First Time Log In process to obtain them.

If you enter the incorrect combination of username and password three times consecutively, the system will lock you out. You must then reset your password using the Forgot Password process.

1. Enter the PCI Apply URL, then press **Enter**.
2. On the Login page, enter your **Username**.

3. Enter your **Password**.
4. Click **Sign In**.

First Time Log In

Use this one-time process to obtain a username and password, if you have not been given them.

1. Enter the PCI Apply URL, then press **Enter**.
2. On the Login page, click **Start Here** under First Time Logging In.
3. In the First Time Login window, enter your full **Merchant Number**.
4. Enter the **Last 4 digits of the Federal Tax ID or SSN** you have on file.
5. Enter your **Two-character state code**.
6. Enter your **ZIP/Postal code**.
7. Click **Continue**.
8. In the Update My Profile window, enter your **Email Address**.
9. Verify your **First Name** and **Last Name**.
10. Enter a **New Password**, and then **Re-enter New Password**.

> Click the show password icon to view the text entered.

11. Select a **Security Question**.
12. Enter your **Security Answer** to the question.
13. Click **Submit** to access PCI Apply.

Retrieve Forgotten Username

Use this process to obtain your username if you have previously logged in but have forgotten your username. Your user name will be sent to your email address.

1. Enter the PCI Apply URL, then press **Enter**.
2. On the Login page, click **Forgot Username**.
3. Enter your **Merchant ID Number** and the **Email** address associated with your account.
4. Click **Continue**.

Reset Forgotten Password

Use the Forgot Password function to obtain a temporary password. A temporary password will be sent to your email address. You can then use that password to log into PCI Apply. You will have to create a new password when you log in.

Temporary passwords are good for 72 hours.

1. Enter the PCI Apply URL, then press **Enter**.
2. On the Login page, click **Forgot Password**.
3. Enter your **Username or Merchant ID Number** and the **Email** address associated with your account.
4. Click **Continue**.
5. Enter the answer to your security question.
6. Click **Continue**.

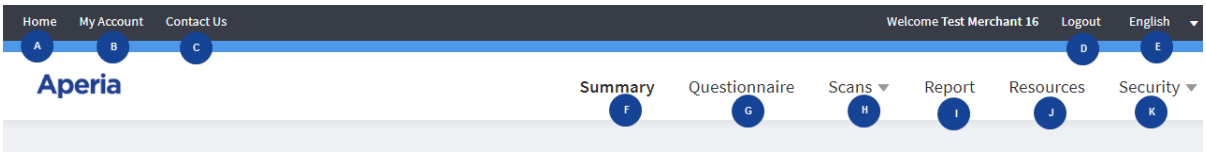
Log Off

Click the **Logout** link on the toolbar.

Navigation and General Functions

Toolbar and Menu

The toolbar and menu displayed at the top of the page provide easy navigation for the site. Some menu options are disabled until you have complete compliance within the application.



A. **Home** takes you back to the landing page.

B. **My Account** enables you to update your login credentials including email, name, password, security question, and security answer.

C. **Contact Us** displays merchant services contact information and provides a form for direct email assistance with the account.

D. **Logout** ends your current session.

E. **Language Menu** enables you to select the language you want to use. The selected language (here it is English) displays as the menu name. Select another language to translate the page.

F. **Summary** takes you back to the landing page.

G. **Questionnaire** takes you to your current questionnaire. This will be inaccessible if your PCI provider identified you as PCI compliant offline.

H. **Scans** menu has options for Network Scan and Endpoint Scanning.

I. **Report** takes you to the Report page where you can access your current and historical compliance documents.

J. **Resources** takes you to a Resource Library with helpful documents, frequently asked questions (FAQs), and a glossary.

K. **Security Bundle** menu has options for the third-party security applications offered by your PCI provider. This menu will not be available if your PCI provider does not offer these services.

General Functions and Appearance

Links to Other Information

Names, IDs, dates, and other information shown in blue text are links to more information. The link may take you to a page with details about the item selected or to a page listing information for the item selected.

Blue text is also used to identify links to additional functionality, such as exporting files or changing settings.

Additional Information Icon

Throughout the application, you will see an Information (**i**) icon next to fields for which you may need more information. Click the icon to display additional information that will help you understand and respond.

Resources

The Resource Library houses tools that will assist you with the PCI process. To access the Resource Library, click **Resources** on the menu.

Click the tabs at the top of the page to navigate through the different sections. Click **X** in the corner to exit the **Resource Library**.

Documents

The Documents tab contains guides to completing the Self-Assessment Questionnaire (SAQ), copies of the questionnaires, and other compliance tools.

1. In the document menu, click the link for the desired content.
   - **Guides**: Contains instruction guides for completing the various SAQs.
   - **Documents**: Contains the official questionnaire documents.
   - **Compliance Tools**: Contains the Device and Inspection Checklist spreadsheet and the Service Provider List Template document.
2. To download a document, click the **Download** link on the desired document.

Education

The Education tab contains educational documents provided by the PCI Council and Aperia, and helpful links to other organizations for further information.

1. In the education menu, click the link for the desired content.
   - **General**
   - **Security**
   - **Fraud**
2. To download a document, click the **Download** link on the desired document.
3. Click any of the Helpful Links to access other websites with additional information.

FAQs

The FAQs (frequently asked questions) tab contains questions commonly asked by merchants and PCI providers.

Click the question or the expand (**+**) icon to view the answer. Click again to close the answer.

Glossary

The Glossary tab contains definitions of commonly used terms.

- Enter a word or phrase in the search field, and press **Enter** to be directed to the correct place in the glossary.
- Click a letter to be directed to the beginning of that section of the glossary. Then scroll to the desired term.

Landing Page

When you log into PCI Apply, you access a landing page. The landing page always shows you the steps required to complete the process and directs you to the next step you need to take.

- If you have not yet started the compliance process, the Welcome Page outlines the five basic steps in the "Let's Get Started' section. Click **Get Started** at the bottom right of the page to start the process.
- If you have started the process, but are not yet compliant, or if you are compliant but need to re-assess, the landing page is Overall PCI Compliance Status. It contains a Status Bar with all the steps in the process. It also contains an indicator with your current status.
    - Click **Continue** or **Re-Assess** to access the step in the process you need to complete.
    - Use the Status Bar links to view or edit a previous page in the compliance process. Sections you have completed have a green check mark. Sections you have partially completed but that have pending tasks are yellow. If further action is needed before you can proceed to the next section, that next section is gray, and you cannot select it.

      If your PCI provider has identified you as PCI compliant offline or as completing your ASV scan with a third party instead of with PCI Apply, then all tabs on the Status Bar will be inaccessible because you did not complete any of the information within PCI Apply.

      If your PCI provider has identified you as an associate merchant whose compliance is completed by another merchant, then the Status Bar will be inaccessible because any changes must be made by the master merchant responsible for your compliance.

- If you are compliant, the Current Reports section displays the reports generated from your most recent compliance. Click **Reports** to access your current and past reports.

  If your PCI provider has identified you as PCI compliant or as completing your ASV scan with a third party instead of with PCI Apply, then reports will be available only if your PCI provider has uploaded them for you.

Merchant Information

The first step in attesting to your compliance is verifying the information in the Merchant Information page. The information on this page was originally entered by your PCI provider. You must review the information, and make any updates or changes needed.

Once you have verified the information, you must read and agree to the terms and conditions before proceeding to the next step.

If you are attesting to compliance for a single merchant ID, then complete only the Verify Your Merchant Information process.

If you are attesting to compliance a master merchant ID and one or more chained merchant IDs, then you must complete these processes in order.

1. Chain Associated Merchants to Your Master Account
2. Verify Your Merchant Information
3. Certify Merchants Chained to Your Master Account

Verify the Merchants Chained to Your Master Account

Perform this process only if your PCI provider has identified your account as a master account with chained merchant IDs. If you are not a master account, go to the Verify Your Merchant Information section.

Your PCI provider may have chained merchants using the merchant relation indicator (MRI) or the tax ID. You must verify the merchant IDs chained to your account.

You can update the merchant name, contact information, and location information for each merchant. You can also remove any merchant ID that does not share the same payment, processing procedures, and security policy as the master account and other chained merchants.

The payment method and processing procedures used across chained merchant IDs do not have to be exactly the same, but they must be substantially the same. For example,

one merchant ID in the chain may use a terminal over dial up and while the other uses a terminal over IP. You must identify that your processing network includes both methods, and you must use the SAQ that applies to the highest level of requirement.

Once you have verified the chained merchant accounts, you can manage them from your master merchant account.

1. Click **Merchant Information** on the status bar of the Overall PCI Compliance Status page or **Get Started** on the Welcome Page.
2. Click the **Show associations** link.
3. If the merchant information needs to be updated, click the Edit Icon (Pencil) for that merchant. Then update any information for the merchant.
4. If a merchant needs to be removed from the chain, click **X** for that merchant from.
5. Click **Continue** to chain the accounts.

Verify Your Merchant Information

1. Click **Merchant Information** on the status bar of the Overall PCI Compliance Status page or **Get Started** on the Welcome Page.
2. Review the Merchant Information section.
   a. Click **Edit** to update or enter any of the information.
   b. Make the needed entries in the Edit Merchant Information window.

      The Contact field must contain both the first and last name of the person responsible for submitting your PCI DSS compliance documents. The full name is required for all compliance reports

   c. Click **Save** to return to Merchant Information.
3. In the Type of Merchant Business section, click the checkbox or checkboxes for your type of business.

   If you select **Others**, you must enter your business type the text box.
4. Select your **Processing Environment**. (If you select **Other**, then you must type a **Description** of your processing environment.)
5. In the Relationships section, click **Yes** or **No** to each of the questions about your business relationships.

6. In the Processing Solution section, enter information about the solutions you use to process credit cards. PCI Apply uses this information to determine the SAQ you need to complete.

   If you know which SAQ you need to complete, you can skip this step. Go to step 6.

   a. Click the button for every solution you use to process credit cards.

      A **Product Code** may be available based on information entered for you by your PCI provider. If so, verify the solution information displayed.

   b. Answer all questions related to the processing solutions selected.

   c. Select your **Processing Solution**. If you select **Other**, then you must type a **Description** of your processing solution.

7. Click **the terms & conditions** link to read them. Then click the checkbox to confirm your agreement to them.

8. Either:

   - Click **Save & Continue** to save your information and proceed to the SAQ appropriate for the processing solution information you entered.
   - At the confirmation message, note the questionnaire selected for you and read the qualifications for this questionnaire. If you qualify for the questionnaire, select the **I agree that the statements above are true** checkbox.

a. Click **Continue**.

   - If you skipped step 5 and know which SAQ you need to complete, click **Select Questionnaire Manually**.

      a. On the Questionnaire Selection page, click the SAQ you need to complete. Then click **Continue**.

      b. At the confirmation message note the questionnaire selected for you and read the qualifications for this questionnaire. If you qualify for the questionnaire, select the **I agree that the statements above are true** checkbox.

      c. Click **Continue**.

Certify Merchants Chained to Your Master Account

Perform this process only if your PCI provider has identified your account as a master account with chained merchant IDs.

When you complete the Merchant Information page, PCI Apply will display a message asking you to certify that all locations (i.e., chained merchant IDs) share the same processing procedures and security policy.

- Click **Yes** to certify that all locations (i.e., chained merchant IDs) share the same processing procedures and security policy. Your questionnaire responses will apply to all your chained merchant IDs.
- Click **No** if there are no related accounts with the same processing procedures and security policy. You must complete the entire compliance process for each merchant ID.

Accept Master Merchant Status

If the master merchant in your merchant chain is changed from another merchant account to your merchant account, you will receive an email informing you of the pending change. You must log to the application to accept becoming the master merchant. The SAQ and ASV status and documents are transferred to your account merchant when you accept master merchant status.

1. Log into the application.
2. At the Accept Master Merchant Status window, review the merchants in the chain.
3. If everything is correct, click **Accept** to become the master merchant.

Questionnaire Selection

You must complete the PCI DSS self-questionnaire required for your business processes. If you know the questionnaire you must use, then you may select it from the Questionnaire Selection page. Or, you can allow PCI Apply to select the appropriate questionnaire for you based on your answers on the Merchant Information page. In this case, the application will bypass the Questionnaire Selection page.

If you are completing the SAQ for a merchant chain, you must use the SAQ that applies to the highest level of requirement in your chain.

Questionnaire Descriptions

Questionnaire A

Questionnaire A applies only to Card Not Present (CNP) merchants. You may use this questionnaire if you:

- Have a website for customers to purchase products/services (also known as E-Commerce). At the point when the customer enters their credit card information, the customer is redirected to another website.
- Use a phone to call a pay-by-phone vendor (also known as an automated 1-800 number) to enter a customer's credit card information.
- Do not store, process, or transmit cardholder data in electronic format.

Questionnaire A–EP

Questionnaire A–EP applies only to E-Commerce merchants. You may use this questionnaire if you:

- Only accept transactions via e-commerce.
- Entirely outsource all processing of cardholder data, except for the payment page, to a third -party payment processor that is approved by PCI DSS;
- Use an e-commerce website that does not receive cardholder data but checks how consumers, or their cardholder data, are redirected to a third -party payment processor validated by PCI DSS;
- Have a website that is operated by a third-party vendor and that vendor is validated for all relevant PCI DSS specifications;
- Originate each element of the payment pages that are delivered to the consumer's browser either from your website or from a PCI DSS service provider;
- Do not store, process, or transmit any cardholder data electronically on your systems or premises, but rely entirely on a third party or third parties to perform these functions;
- Have confirmed that all third parties storing, processing, and/or transmitting cardholder data are PCI DSS compliant;

This questionnaire requires an ASV scan of your network.

Questionnaire B

Questionnaire B applies to merchants using imprint machines or stand-alone dial out (analog) terminals. You may use this questionnaire if you:

- Use a credit card terminal or machine connected by a phone line/fax line.
- Manually enter or swipe credit card information on a device such as a smartphone or tablet connected by a data plan or mobile hot spot.
- Use a manual card reader to take an imprint of the card and calls in to receive voice authorization on the card.
- Use a wireless credit card terminal or machine that relies on a cellular technology.
- Do not store card holder data in electronic format.

Questionnaire B–IP

Questionnaire B–IP applies to merchants who use stand-alone IP connected terminals. You may use this questionnaire if you:

- Use a credit card terminal or machine connected by Ethernet internet.
- Use a credit card terminal or machine connected by Wi-Fi internet.
- Use a credit card terminal or machine on a Voice over IP connection.
- Use a credit card terminal or machine connected by DSL to the internet.
- Do not store card holder data in electronic format.

This questionnaire requires an ASV scan of your network.

Questionnaire C

Questionnaire C applies to merchants with payment application systems connected to the internet. You may use this questionnaire if you:

- Use a point of sale (POS) software on a computer.
- Manually enter or swipe credit card information on a device such as a smartphone or tablet connected by Wi-Fi.
- Have a POS environment whose physical location is not connected to other locations or premises, and any LAN is only for one single store.
- Use an online payment website or virtual terminal, log in with a username and password, and swipe the credit card information.
- Do not store card holder data in electronic format.

This questionnaire requires an ASV scan of your network.

Questionnaire C–VT

Questionnaire C–VT applies to merchants with web-based virtual terminals. You may use this questionnaire if you:

- Access the PCI DSS compliant virtual payment terminal solution via a computer that is isolated in a single location and is not connected within your network to other locations or systems.
- Do not have any hardware devices attached to your company's computer that are used to capture or store cardholder data.
- Will not otherwise receive or electronically transmit cardholder data via any channels.
- Do not store card holder data in electronic format.

Questionnaire D

Questionnaire D applies to merchants who stores full length credit card information in encrypted format on a computer, hard drive, USB, or any other electronic device.

This questionnaire requires an ASV scan of your network.

Questionnaire P2PE

Questionnaire P2PE applies to merchants using only an approved PCI Point-to-Point Encryption Solution. You may use this questionnaire if you:

- Have **all processing of payments** validated through a PCI P2PE solution approved and listed by PCI SSC.
- Do not have any legacy storage within the environment of electronic cardholder data.
- Do not store card holder data in electronic format outside of their P2PE solution.
- Have implemented the P2PE solution in accordance with the solution's instruction manual.

Select a Questionnaire

1. Access the Questionnaire Selection page by:
   - Clicking **Select Questionnaire Manually** on the Merchant Information page.
   - Clicking **Questionnaire Selection** on the status bar at the top of any page.
2. Click anywhere within the box for the desired questionnaire.

3. Click **Continue**.
4. Select the **Service Provider** and **Enter Service Name** for your credit card processing software.
5. If you use more than one, select the **Add additional** link to add another service provider.
6. Click **Continue**.
7. At the confirmation message, note the questionnaire selected and read the qualifications for this questionnaire. If you qualify for the questionnaire, select the **I agree that the statements above are true** checkbox.
8. Click **Continue**.

Questionnaire

Use the Questionnaire page to complete the SAQ you selected or that was selected for you by PCI Apply.

To be compliant, you must take the steps necessary to be able to answer Yes to each question of each part of the SAQ. If you answer No to any question, then you must correct the deficiency. Once corrected, return to the question and update your answer to Yes.

You may answer N/A to any requirements not applicable to your environment, but you must provide an explanation for why the requirements do not apply.

Questionnaire Status

Your questionnaire status appears to the right of the questionnaire title.

Questionnaire Compliance Status	Description
Not Started	You have not yet selected a questionnaire
In Progress	You have entered some answers, but the questionnaire is still incomplete.
Non-Compliant	Some answers you provided on the questionnaire are out of compliance.
Not Signed	The questionnaire is complete, but you have not reviewed and signed it.

Questionnaire Compliance Status	Description
Compliant	Within the past year, you have completed, reviewed, and signed the questionnaire.
Expired	You completed the questionnaire over a year ago and it is now expired. You need to re-assess.

Complete a Summarized Questionnaire

If you are a non-scanning merchant, your PCI provider may have selected a summarized questionnaire for you. The summarized questionnaire enables you to acknowledge all statements within a section are true, rather than responding to each individual question.

1. On the Questionnaire page, click **Start Questionnaire** to proceed.
2. For each section, review the statements, then click the **I attest that I have read and adhere to the requirements in this section** checkbox.
3. Click **Continue** to proceed to the next section.
4. Once you have completed all the sections, click **Continue to Scan**.

Complete a Full Questionnaire

1. On the Questionnaire page, click **Start Questionnaire** to proceed.
2. At the section overview read the general information, and then click **Start Section**.
3. Respond to each question.
    a. Hover over the Information icon next to any question to review a tip with more information about the question being asked.
    b. Select the appropriate button to answer the question.
        - If you select **Yes**, continue to the next question.
        - If you select **Yes with CCW**, then a Compensating Controls Worksheet window will appear. Answer all questions, then click **Submit**.
        - If you select **No**, then select your **Stage of Implementation** and **Estimated date of completion**. Then select **Save**.
        - If you select **N/A**, then respond to **Please specify why this question is not applicable** and select **Save**.
4. After answering all questions, click **Continue** to proceed to the next section.
5. Repeat steps 2 through 4 for each section.

6. Once you have completed all the sections, click **Continue to Scan**.

   If an ASV scan is not required, PCI Apply bypasses the **Network Scan** tab and takes you to the **Review and Sign** page after you complete all sections of the questionnaire.

Network Scan

An ASV scan of your network is required every 90 days if your business processing method requires a scan. Scans can take some time to complete so you should launch the scan prior to the expiration date.

Some examples of processing methods that require an ASV scan include:

- A-EP Website using a direct post
- B-IP Terminal connected to an internet source (Ethernet cable)

ASV scans are required for each public-facing IP address or domain name of the network you use to process credit cards. The IP addresses or domain names are known as scan targets.

Scan Process

This is the general process for scanning the network and becoming compliant. The tasks in this process that you must perform in PCI Apply are described in the sections below. While working in PCI Apply, you can review this information by clicking on the **How to achieve ASV Compliance** link on the Network Scan page.

1. Identify all scan targets.
   - You are responsible for identifying all in-scope scan targets.
   - All internet-facing systems of your card-processing network must be identified as IP addresses or domain names.
2. Add scan targets. This is done on the Network Scan Summary Target Management page.
3. Launch scans against targets.
   - Scanning all your scan targets at one time is not necessary. Depending on your vulnerability management policy, you may choose to scan some targets more often than others.
   - Multiple passing scans can be combined for use in quarterly ASV compliance.

- All the scan targets included in your compliance request will expire at the same time, regardless of the individual scan dates.

4. Remediate issues or request exceptions.
   - If issues were found which initially caused a failed scan, you can remediate the issues or request exceptions.
   - Remediated issues must be confirmed by a rescan.
   - Exceptions can be requested for disputed issues.
5. When all in-scope targets have a passing scan, submit an ASV compliance request.
   - Multiple scan results can be submitted in a compliance request.
   - All scans must be less than 90 days old.
6. The ASV Team will review your submitted compliance request.
   - Always allow 1-2 business days for review and approval.

ASV Compliance Status

Your ASV scan status is shown in the ASV Compliance Status section of the Network Scan Summary page. This table contains the statuses, in life-cycle order, and their descriptions.

ASV Compliance Status	Description
Not Started	You have selected an SAQ that requires a scan, but the scan has not yet been launched.
Non-Compliant	Your scan has been started, but you have not completed all the steps necessary to achieve a Compliant status. The most common reason for this is that you have not addressed failing issues in your scan.
Compliant	Your ASV Compliance request has been approved by the ASV team within the compliance period (90 days).
Expired	You have had a previously approved ASV Compliance request, but it is now out of the compliance period (more than 90 days).

Enter Your Scan Targets

The PCI DSS requires that you provide an IP address for all externally accessible, internet-facing interfaces that can be used to access your card processing network.

Enter the IP addresses or domain names that must be scanned. You must provide fully qualified domain names that are entryways to your card processing network. These include, but are not limited to:

- Domains for web servers
- Domains for mail servers
- Domains used in name-based virtual hosting
- Web server URLs to hidden directories that cannot be reached by crawling the website from the home page
- Any other public-facing hosts, virtual hosts, domains or domain aliases

During the scan, a scan target entered as a domain name will be resolved to the IP addresses associated with that domain. Scan status is reported by individual IP address.

You can have up to 50 scan targets in your IP address/domain name pool. Your targets are not saved within the application until they appear in the IP Address/Domain Name Pool of the Target Management window.

You can enter your scan targets manually, or you may import them using a CSV or text file. Scan targets may be an IPv4 or IPv6 address, a range of IP addresses, or a domain name.

Manually Enter Scan Targets

1. On the Network Scan page, click **Add Scan Target**, to enter your first scan targets, or **Manage Scan Targets**, if you have previously entered scan targets.
2. In the Input section, type an IP address or domain name.
3. Press **Enter** to enter another scan target.
4. Once you have correctly entered all your scan targets, click **Add**.
5. At the confirmation message, review your list of targets. Click the checkbox for **I confirm that I have permission to launch scans against these scan targets**.
6. Then click **Continue**. Your scan targets will be listed in the IP Address/Domain name pool section.
7. Click **Return to Network Scan Summary**.

Import Scan Targets

You can import your scan targets using either the .csv or .txt file template available for download.

The import process will import up to 50 targets from a file, depending on whether you have any scan targets in your pool. The process imports scan targets in order from file until either all are imported or there are 50 in the pool.

The maximum size of the imported file is 10 MB.

1. On the Network Scan page, click **Add Scan Target**, to enter your first scan targets, or **Manage Scan Targets**, if you have previously entered scan targets.
2. In the Input section, click the **Import From File** link.
3. Click the **Download** link for the CSV or text sample file.
4. Enter your IP addresses or domain names in the file and save it.
5. Select **Browse**, then search for and select your file.
6. Click **Import**.
7. At the validation message, if they imported successfully, click **Continue** to proceed.

   If there are issues, correct them in the file and then try importing again.
8. Verify the imported scan targets in the Input section. Click **Add**.
9. Then click **Continue**. Your scan targets will be listed in the IP Address/Domain name pool section.
10. Click **Return to Network Scan Summary**.

Verify Scan Targets

If you enter scan targets as a domain address or an IP range, you must verify the IP address in that domain or range.

Verify IP Addresses in a Domain

1. Select scan targets from the identified domains.
   a. In the Domain Associates to Multiple IP section, click **Select Option** for a domain to display the Domain with Multiple Associated IPs Confirmation window.

b. In the Domain with Multiple Associated IPs Confirmation window, either:

- Confirm that all IP addresses associated with the domain are identical by clicking **I confirm that the web application is identical at each IP address. I request a single associated IP address be scanned.**
- Scan all associated IPs by clicking **I cannot confirm that the web application is identical at each IP address. I request all associated IPs be scanned.**

c. If you have additional domains to confirm, click the **Open next domain** checkbox.

d. After confirming all domains, click **Confirm**. This returns to the Target Verification Results window, and the confirmed domains display in the Selected Targets section.

2. In the Individual Targets section, click **Select** for each individual IP address you want to scan. The selected IP addresses display in the Selected Targets section.
3. After all scan targets are confirmed and added to the Selected Targets section, click **Add**.

   This returns to the Target Management page, and the selected scan targets appear in the IP Addresses/Domain Names Pool.

Verify IP Addresses in a Range

1. Select scan targets from the identified IP address ranges.

   a. In the IP Ranges section, click **Confirm** to confirm the number of IPs in an IP range.

   b. In the IP Range Confirmation window, review the IP addresses within the range. Then either:

   - Click **Dismiss** if you do not want to include these IP addresses.
   - Click the **Open next IP Range** checkbox or click **Confirm** if you have reviewed all the IP ranges. This returns to the Target Verification Results window, and the confirmed IP addresses display in the Selected Targets section.

2. In the Individual Targets section, click **Select** for each individual IP address you want to scan. The selected IP addresses display in the Selected Targets section.
3. After all scan targets are confirmed and added to the Selected Targets section, click **Add**.

   This returns to the Target Management page, and the selected scan targets appear in the IP Addresses/Domain Names Pool.

Identify the Scan Targets in the Scan Scope

You must identify the scan targets that are within the scope of the scan you are preparing to launch. Only the scan targets within the scope will be scanned. Scan targets that are marked out of scope will not be included when you launch a scan or when a scan is launched by the scheduler.

You are responsible for defining the appropriate scope of your scan and providing all your internet-facing IP addresses and domain names for scanning. You are responsible if an account data compromise occurs via an externally facing system component that you did not include in your scan scope.

1. On the Target Management page, in the IP Address/Domain Name Pool section, scroll to the right.
2. Identify the status of each scan target in the pool by clicking the link in the Action column.
   - **Add to Scope**: Use to identify IP addresses currently in your network that need to be scanned.
   - **Delete**: Use to remove unscanned scan targets from the IP address pool. You cannot delete targets that have previously been scanned.
   - **Remove from Scope**: Use to remove previously scanned targets from the scope of the current scan. Remove from the scope any IP addresses that are no longer part of your card processing network or are no longer public facing and therefore no longer need to be scanned. These IP addresses remain in the pool for historical purposes.

     Removing an IP address will not change its current status but will remove it from future scans.
3. Once the scope is correct, click **Return to network Scan Summary**.

Launch an ASV Scan

After you have entered and verified your scan targets, you can initiate the scan.

1. On the Network Scan Summary page, click **Launch Scan** to proceed.

2. If multiple IPs associated with one domain are selected, the Verifying Confirmation window will display.
    - Select the **I confirm that the web application is identical at each IP address. I request a single associated IP address be scanned** radio button to launch a scan for only the first IP in this list.
    - Select the **I cannot confirm that the web application is identical at each IP address. I request all associated IP addresses be scanned** radio button to launch a scan for all IPs in this list.
3. Click **Confirm** to launch the scan.
4. At the confirmation message, click **Close**. The scan may take up to two business days to complete.
5. The Network Scan Summary now contains a Scan Target Status Summary section and a Scan Result by Status section. Use these sections to monitor the progress and results of your network scan.

Individual Target Status	Description
Not Started	The target has never been scanned.
Queued	The target has recently had a scan launched that is waiting to be executed.
Actively Scanning	A scan is actively running against this target.
Compiling Scan Results	A scan has recently completed, and scan results are being compiled into scan reports.
Fail – Action Needed	The target has failing vulnerabilities in their latest scan result.
Action Required	The target has an Inconclusive note in its latest scan result. You must provide additional confirmation information for the scan target to pass.
Pass	The target has no failing vulnerabilities in its latest scan result.
Expired	The target has a Pass or Fail – Action Needed result, but it has been over 90 days since the Scan Completed Date. The target has an Action Required result, but it has been over 30 days since the Scan Completed Date.

Schedule Scans

You can use the Scan Scheduler function to launch a scan for targets on a specific date or to launch recurring scans on a set frequency. Frequent scanning can be an effect part of your vulnerability management process. Frequent scans help ensure you are aware of any new vulnerabilities in your network so that you can address them quickly.

You can only have one schedule at time.

Once you schedule a scan, the next scheduled scan date displays in the Scan Target Status Summary section. The targets which now have a scheduled scan will have the frequency specified in Scheduled column of the Scan Result by Status section.

Schedule Scans on Specific Date

Use this process to schedule a scan to automatically launch on a specific date.

1. On the Network Scan Summary page, click **Create Schedule** to open the Scan Scheduler.
2. Click the checkbox for each IP address or domain name you want to include in the scan.
3. Click **Next**.

   If you select or deselect a domain that is associated with multiple IP addresses, all the associated IP addresses will be selected or deselected.

4. In **Frequency**, select Specific Date.
5. In **Scan On**, select the desired date. The date must be at least 72 hours from the previous scan.
6. Click **Submit** to create the schedule for the next scan. The scheduled scan date appears in the Scan Target Status Summary section on the Network Scan Summary page.

Schedule Recurring Scans

Use this process to schedule recurring scans on a weekly, monthly, or quarterly basis. The schedule includes five scans, regardless of frequency.

1. On the Network Scan Summary page, click **Create Schedule** to open the Scan Scheduler.
2. Click the checkbox for each IP address or domain name you want to include in the scan.
3. Click **Next**.

> If you select or deselect a domain that is associated with multiple IP addresses, all the associated IP addresses will be selected or deselected.

4. Select the **Frequency** of recurrence.
5. In **Scan On**, select the desired recurrence for the selected frequency.

> If you selected Quarterly, the next five scan dates are calculated and displayed.

6. Click **Submit** to schedule the recurring scans. The next scheduled scan date appears in the Scan Target Status Summary section on the Network Scan Summary page.

Edit a Scan Schedule

You can edit or delete the scan schedule.

1. On the Network Scan Summary page, click the **Next Scheduled Scan** date link to open the Scan Scheduler Summary.
2. Click **Edit Schedule**.
3. In the Scan Scheduler, select or deselect the checkbox for each IP address or domain name you want to include in the scan.
4. Click **Next**.

> If you select or deselect a domain that is associated with multiple IP addresses, all the associated IP addresses will be selected or deselected.

5. Select the **Frequency** and **Scan On** for the desired recurrence.
6. Click **Submit** to schedule the recurring scans. The next scheduled scan date appears in the Scan Target Status Summary section on the Network Scan Summary page.

Disable a Schedule

1. On the Network Scan Summary page, click the **Next Scheduled Scan** date link to open the Scan Scheduler Summary.
2. Click **Disable Schedule**.

Launch a Scan for Targets with Scheduled Scans

You can manually launch a scan for targets that have been scheduled for a scan.

If you launch a new scan within 72 hours before the next scheduled scan date, PCI Apply will cancel the next scan date. If you set the scan for a specific date and not a recurring frequency, the schedule will be deleted.

1. On the Network Scan Summary page, click **Launch Scan**.
2. In the Launch Scan window, click the checkbox for each IP address or domain name you want to include in the scan.
3. Click **Launch Scan**.

Respond to the Scan Results

Even if your initial scan result is something other than Pass, you may still be able to use the scan for your quarterly ASV compliance. You can fix failing vulnerabilities and then rescan the failing targets or a failing vulnerability may be eligible for an exception.

You must respond to each failure promptly. All scan targets must pass before the end of your 90-day period.

Respond to Fail – Action Needed Status

You must resolve all failing vulnerabilities in a scan before the scan target will have a status of Pass. A permanent solution may involve applying a patch or modifying configuration to resolve the vulnerability. If you remediate the issue, you must rescan to confirm that the vulnerability is no longer present.

Some vulnerabilities may not be resolvable but may be eligible for an exception. The PCI council requires that all exceptions must expire after 90 days. The exception is a temporary measure that expires after 90 days.

When you request an exception, the ASV Team assigns it a case number and gives it the status of Pending ASV Team Action. The ASV Team will respond to the request by either

granting it (if possible) or requesting additional information, such as screen shots from the system you are using.

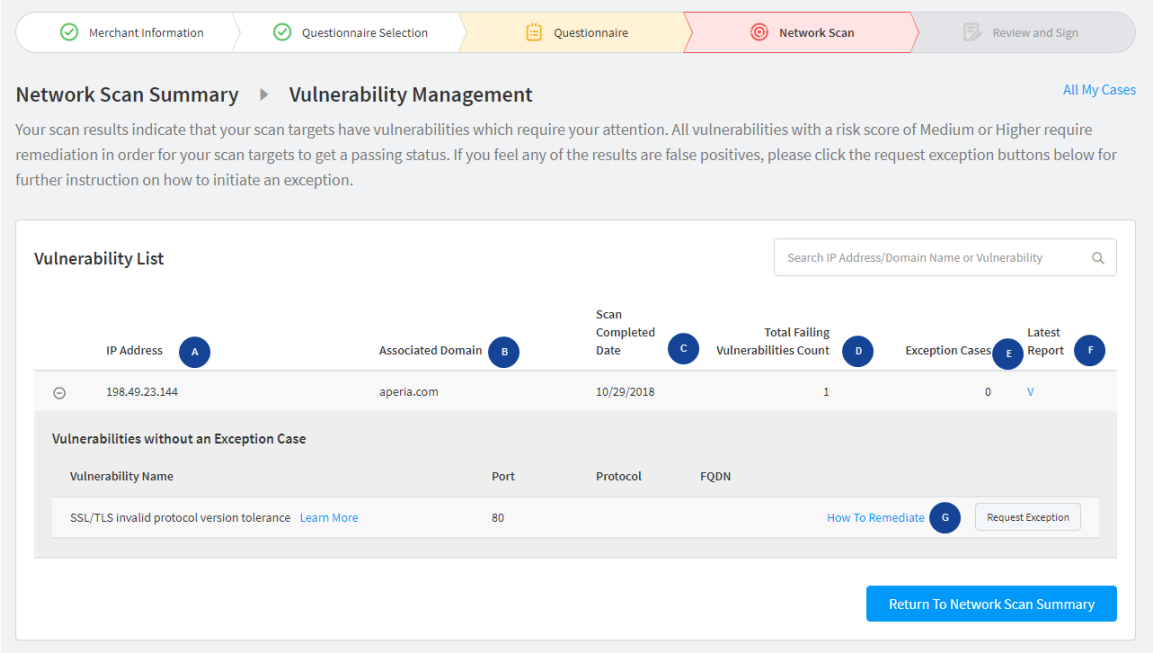
Open exception cases are listed in the Vulnerabilities with an Exception Case section of the Vulnerability Management page. Each case entry will include the case number and status.

If an exception case's status is changed to Pending Scan Customer Action, you may need to enter additional information in the case to provide further explanation or evidence supporting the exception request. Once you submit additional information, the case status will change back to Pending ASV Team Action.

If the ASV team grants the exception, they will close your exception case. When the exception case is closed, the vulnerabilities in that case are no longer failing issues so they do not impact the target status.

Access Guidance on How to Respond

1. On the Network Scan Summary, click the **Vulnerability Management** link to open the Vulnerability Management page.



2. In the Vulnerability List, for each vulnerability, click the **Learn More** link. For many common vulnerabilities, the ASV Team has provided recommendations on the best way to move forward.

3. Click the **How To Remediate** link to access instructions on how to remediate the specific vulnerability.
4. On the Solutions window, click either **Export to Word** or **Export to PDF** to export the instructions.
5. Click **X** to return to the Vulnerability Management page.
6. If possible, follow the recommendations and remediation instructions, then follow the instructions to rescan the failing scan targets.
    - When all failing vulnerabilities have been resolved a scan target status will change to Pass.
    - If necessary, request an exception using the instructions below.

Request an Exception

Only you submit an exception request. This cannot be done for you by a customer service representative.

1. On the Network Scan Summary, click the **Vulnerability Management** link to open the Vulnerability Management page.
2. In the Vulnerability List, click **Request Exception** for the vulnerability you cannot remediate.
3. On the Vulnerability Exception Request page, in the Vulnerability Exception section, review the information for the vulnerability for which you are requesting an exception case.
4. In the Unrequested Vulnerabilities section, review information for other vulnerabilities which are associated with the same target but for which you have not yet requested exception cases.

    If appropriate, click the **+** displayed next to a vulnerability to add it to the Vulnerability Exception section and the exception case.
5. In **Add New Comment**, type an explanation for requesting the exception case.
6. If needed, click **Attach File** to upload a supplementary file.
7. Either:
    - Click **Save** to save the progress and submit later
    - Click **Attest and Submit** to open the Submit Exception Case Confirmation window. Then click **Confirm** to submit the exception request for ASV team review.

Enter Additional Information on an Exception Case

If an exception case's status is changed to Pending Scan Customer Action, you may need to enter additional information in the case to provide further explanation or evidence supporting the exception. Once you submit additional information, the case status will change back to Pending ASV Team Action.

Repeat this process until either the exception can be granted, or you are able to resolve the vulnerability without needing an exception.

1. On the Network Scan Summary, click the **Vulnerability Management** link to open the Vulnerability Management page.
2. Click the exception case number (EC#) link to open the Exception Case window.
3. Enter additional explanation or evidence to support the exception. You can
   a. Enter additional information in the Comment section.
   b. Attach a document, if needed.
   c. Click **Attest** to submit the information. Once submitted, the status will change back to Pending ASV Team Action.

Respond to Action Required Status

The Action Required status indicates that the scan result cannot be provided until you provide additional confirmation. In many situations, once you have provided confirmation that the scan was performed under valid conditions and that it was not actively blocked, then the scan can be used as a Passing scan.

If you modify the scan target rather than responding to the inconclusive note, then you need to launch another scan.

Review an Inconclusive Scan

1. On the Network Scan Summary page, in the Scan Result by Status section, click **Respond** for the scan target with the status Action Required.
2. In the Inconclusive Scan window, review the conditions that may have resulted in the inconclusive scan. For each statement:
   - Click **Yes** for a statement to attest that you agree it is correct.
   - Click **No** for any statement to which you cannot attest to its correctness. This displays a message with additional information regarding the risk to your network.
3. When you have responded to all statements, then click **Submit**.

4. On the Network Scan Summary page, the Scan Result by Status section displays the status of the scan target.
    - The status will be Pass if you responded Yes to all statements.
    - The status remains Action Required if you responded No to any statement. The associated action button will be **Unresolved**.

ASV Compliance Request

Submit your ASV compliance request to the ASV Team when all your scan targets have the status Pass or Pass with Special Notes. Submitting the compliance request, which attests to the validity of your entire compliance request, is the final task in completing your ASV scan.

When the scan engine detects non-critical risks associated with a specific scan target, it assigns that scan target a status of Pass with Special Notes. You will be asked to respond to these special notes when you submit your ASV compliance request.

In your compliance request, you identify whether your network uses load balancers and, if so, whether they are configured identically. A load balancer divides work over two or more computers to reduce processing time. Load balancing may be done with hardware, software, or both.

Your ASV compliance request must be reviewed and approved by the ASV Team. Once your request is approved, your status changes to Compliant. The compliance duration of the request is 90 days from the earliest scan completion date for the scan targets in the request.

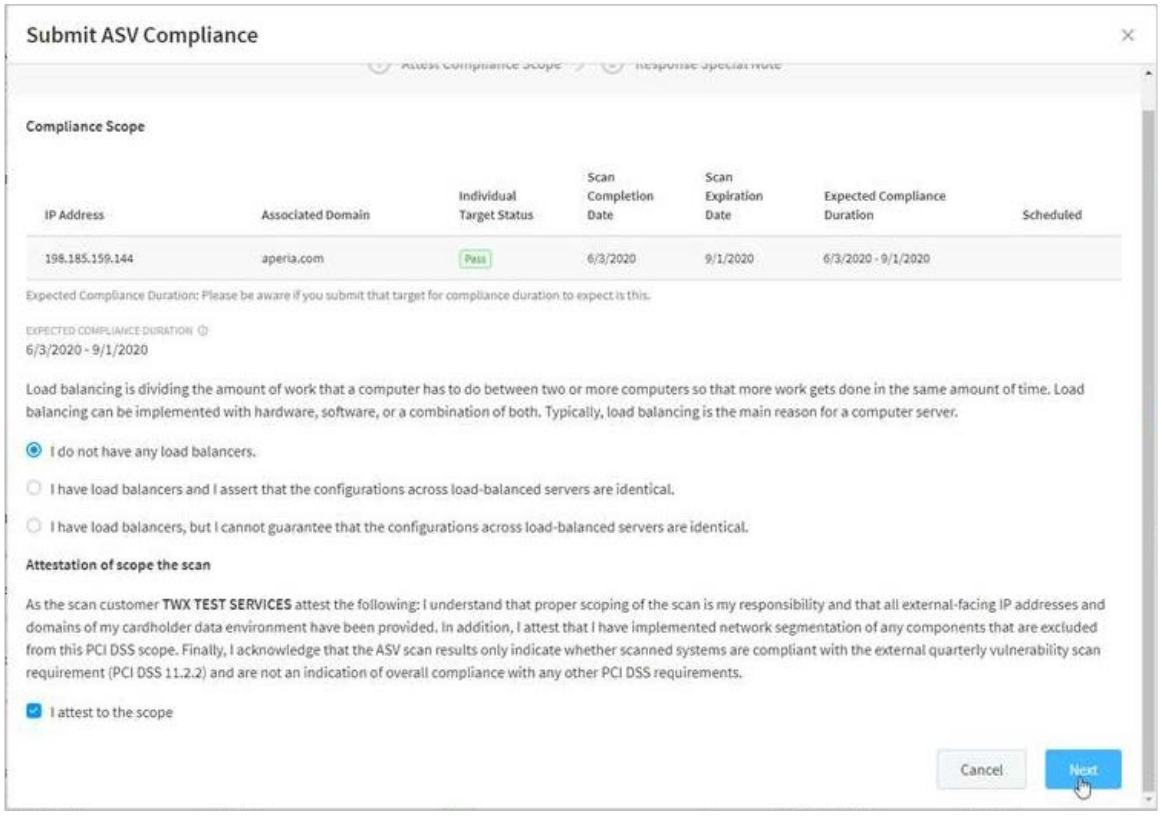
Submit an ASV Compliance Request

When you submit your ASV compliance request, you are attesting to the validity of your entire compliance request by confirming the scope and the validity of all supporting evidence.

1. On the Network Scan Summary page, in the Scan Target Status Summary section, click **Submit ASV Compliance**.

    This button is enabled only when all the scan targets that are in scope have a status of Pass.

2. In the Submit ASV Compliance window, in the load balancer section, click the radio button for the load balancing statement that applies to you.



3. Click the **I attest to the scope** checkbox to attest to the scope of the scan.
4. Either:
   - Click **Submit** If all the scan targets have a status of Pass, this submits the request for ASV compliance and returns to the Network Scan Summary page. This completes this task.
   - Click **Next** if any of the scan targets have a status of Pass with Special Notes, this accesses the Response Special Note tab of the Submit ASV Compliance window. You must continue to the next step.
5. For each IP address with a special note, click **Respond** to open the Special Note window.
6. On the Special Note window,
   a. Click the checkbox confirming the software, hardware, or other condition is required and implemented securely.
   b. Click **Submit** to return to Response Special Note tab of the Submit ASV Compliance window.
7. Repeat steps 5 and 6 for every IP address with a special note.

8. After addressing all special notes, on the Submit ASV Compliance window, click **Submit** to submit the request for ASV compliance.
9. On the ASV Compliance Request Details window, click **Close** to return to the Network Scan Summary page.

Review Your Compliance Request

Until your ASV compliance request is processed, you can review it if needed. On the Network Scan Summary page, click the **Your ASV Compliance request has been submitted** message to open the ASV Compliance Request Details window.

The ASV Compliance Request Details window displays the submission date of the request, a list of the scan targets included in the request, and each scan target's scan completed date.

Respond to a Declined Compliance Request

If your ASV Compliance request is declined by the ASV Team, the Network Scan Summary page will display the **Your ASV Compliance request has been declined** message.

Your request may be declined if the manual review by the ASV Team identifies a problem, such as your scan was more than 90 days old or if an invalid scan target was submitted. The ASV Team will have set the status of one or more targets to fail and will use it to note the cause of the failure. You must review the request to determine why it was denied, correct the issues, and submit a new request.

1. On the Network Scan Summary page, click the **Your ASV Compliance request has been declined** message to open the ASV Compliance Request Details window.
2. Address the issue identified in the ASV Comment column on the failed target or targets.
3. After addressing all issues, identify the scan targets that are in scope and launch another scan. Follow the normal process to respond to the new scan's results and to submit an ASV compliance request.

Download Your Compliance Reports

The Network Scan Summary page will display your ASV Compliance status as Compliant once your request is approved by the ASV Team. A note beneath the status shows the number of days until your compliance expires.

Once your status is Compliant, you can download your compliance reports.

- Attestation of Scan Compliance
- Executive Summary
- Vulnerability Details

Download the Attestation of Scan Compliance Report

1. On the Network Scan Summary page, click the **View Details** link to open the ASV Compliance History window.
2. On the ASV Compliance Details window, click the **A** link to download the Attestation of Scan Compliance report.
3. For the desired request date, click the Expand icon to view further details about the scan targets included in the compliance request.

Download the Executive Summary and Vulnerability Details Reports

You can download the Summary and Vulnerability Details reports from the Scan History window. You can also view a list of all the IP addresses included in a scan.

1. On the Network Scan Summary page, in the Scan Target Status Summary section, hover over **View History** and click **Scan History**.
2. For the desired scan date, click the **E** link to download the Executive Summary report.
3. For the desired scan date, click the **V** link to download the Vulnerability Details report.
4. For the desired scan date, click the Expand icon to show the details of the IP addresses included in the scan.

Review and Sign

The last step in completing PCI compliance is to review and sign the questionnaire. You will automatically be directed to this page after completing the questionnaire or the scan, if required, or you can navigate to this page by clicking **Review and Sign** on the Status Bar.

The Review and Sign page is an overview of the merchant information and payment processing information you entered. You must review this information, and make any corrections, if needed. Then you must confirm your compliance, electronically sign the questionnaire, and submit it.

Review and Sign Your Compliance Questionnaire

1. On the Review and Sign page, review the content of each section.
2. If a section has incorrect information, click **Edit** to make the changes.
3. In the Confirmation of Compliance section, click the checkbox for each statement to confirm your compliance with it.
4. In the PCI DSS Validation section, enter your Merchant Executive Officer Name, Title, and Last 4 Digits of Your Tax ID or Social Security number.

   This is your electronic signature, and it is as legally binding as your signature on a paper document.

5. Click **Submit** to complete your compliance submission. This accesses the Report page where you can view, download, or print your compliance reports.

Get Your Site Seal

Once you achieve PCI compliance, you can download your site seal. You can display the site seal on your website to show your customers that you are compliant and that their credit card information is secure.

1. On the Overall PCI Compliance Status page, click **Get Site Seal**.
2. On the Site Seal Modal, in the Seal Code section, click **Copy Seal Code to Clipboard**.
3. This opens the Windows Clipboard with the HTML code. Save the file. You can then use the HTML code on your website.

Reports

PCI Apply generates several reports as you complete the compliance attestation process. These reports are available from PCI Apply for at least three years, as required by the PCI council.

If desired, you may use the Reports page to download or print a copy of your PCI documents to file for your company records.

1. On the menu, click **Report**.
2. For the desired report, click **Report** to select the current or previous instance of the report.
3. Click **View/Print** to download a copy of the report.
4. Click **Email** to send a copy of the report via email for future reference.

Additional Security Services

Your PCI provider may offer you additional security services that help secure your network and devices and reduce the likelihood that your network and devices will be compromised, and confidential data will be exposed. If your PCI provider does not offer these services, they will not be available on the PCI Apply menu.

Endpoint Management

Cyberforce Endpoint Management is a lightweight agent that utilizes cutting edge technology to monitor the health and security of endpoint devices (computer, laptop, tablet). This agent protects an endpoint device by ensuring its operating system and applications are properly patched and configured so they are not susceptible to attacks by hackers and other bad actors.

1. On the menu, point to **Security Bundle**, the click **Endpoint Management**.
2. Enter the **First Name**, **Last Name**, and **Email** address of the administrator user.
3. Click **Order Licenses**.
4. Enter the **First Name**, **Last Name**, and **Email** address of the user who will serve as the manager for the account.
5. Enter the **Total Licenses** needed.
6. Click **Order**.

Endpoint Protection

CylancePROTECT applies artificial intelligence and machine learning to instantly identify and prevent malware and cyberattacks on the host machine.

To use this service, you must identify the account administrator user for your organization. Credentials and access information will be sent to the email address you enter for the account administrator.

1. On the menu, point to **Security Bundle**, the click **Keystroke Encryption**.
2. Enter the **First Name**, **Last Name**, and **Email** of the user who will serve as the ACS user.
3. Click **Get Started**.

Keystroke Encryption

EndpointLock™ is a keystroke encryption layer that is installed on your peripheral devices to protect information at the point of data entry. Keystroke encryption blocks all keylogging malware and prevent further intrusion into the network.

To use this service, you must identify the Advanced Cyber Security (ACS) user for your organization. Credentials and access information will be sent to the email address you enter for the ACS user.

1. On the menu, point to **Security Bundle**, the click **Keystroke Encryption**.
2. Enter the **First Name**, **Last Name**, and **Email** of the user who will serve as the ACS user.
3. Click **Get Started**.

Endpoint Scanning

Aperia endpoint scanning provides the ability to conduct the following scans on a network endpoint.

- Security Scan: Reviews the endpoint for security violations and to ensure that it is properly patched. Provides guidance on how sever the issues are and how to fix them.
- PAN Scan: Uses the MOD 10 algorithm to identify unencrypted card numbers that are stored on the device.

- PII Scan: Identifies potential personally identifiable information, such as driver licenses and Social security numbers that are stored on the device in an unencrypted manner.

Scan a Device

You must be logged into PCI Apply on the device you want to scan.

1. On the menu, point to **Scans** or to **Security Bundle**, the click **Endpoint Scanning**.
2. Click **Scan Now** for the scan you want to run.

Send a Scan Inquiry to Another Device

You can send an email to other users in your network so that they can initiate endpoint scans on their devices.

1. On the menu, point to **Scans** or to **Security Bundle**, the click **Endpoint Scanning**.
2. Scroll down to the Send Scan Inquiries section, then select the checkboxes for the scans you want run on the target device.
3. Type the **Email** address of the person who will run the scan on the target device.
4. Type a Subject for the email. The subject should identify the source and purpose of the email so that users can identify it as legitimate.
5. Type a **Message** explaining what actions you want the user to take. The application adds links for the selected scans to the email, but it does not provide any other information.
6. Click **Send**.

Data Breach Protection

Data breach protection provides merchants with access to incident response, legal counsel, cyber forensics, security consulting, and loss protection service for the management and remediation of regulatory infractions related to a data breach.